第4層流量監控器如何阻止流量？

問題：

如果第4層流量監控器僅接收映象流量，它如何阻止流量？

環境：

第4層流量監控器 — L4TM配置為阻止可疑流量

解決方案：

思科網路安全裝置(WSA)具有內建的第4層流量監控器(L4TM)服務，可以阻止所有網路連線埠(TCP/UDP 0-65535)上的可疑作業階段。

為了能夠監控或阻止這些會話流量，必須使用TAP（測試訪問埠）裝置或通過配置網路裝置的映象埠（思科裝置上的SPAN埠）將流量重定向到WSA。尚不支援L4TM串聯模式。

即使流量僅從原始會話映象（複製）到裝置，WSA仍可以通過休眠TCP會話或為UDP會話傳送ICMP「主機無法到達」消息來阻止可疑流量。

對於TCP會話

當WSA L4TM收到來自或發往伺服器的封包，且流量與封鎖行動相符時，L4TM會根據不同的情境向使用者端或伺服器傳送TCP RST（重設）資料包。TCP RST資料包只是TCP RST標誌設定為1的正常封包。

RST的接收方首先對其進行驗證，然後改變狀態。如果接收器處於LISTEN狀態，則會忽略它。如果接收器處於SYN-RECEIVED狀態並且先前處於LISTEN狀態，則接收器將返回到LISTEN狀態，否則接收器將中止連線並進入CLOSED狀態。如果接收方處於任何其他狀態，它將中止連線並通知使用者並進入CLOSED狀態。

有兩種情況需要考慮（兩種情況下使用者/客戶端都位於防火牆之後）：

第一類是可疑資料包從防火牆外部傳入內部網路中的客戶端時。RST將傳送到伺服器，在這種情況下，它將到達防火牆，通常不會轉發RST，但會終止會話，因為它會認為RST實際上來自客戶端。在此案例中，RST的來源IP將是使用者端的偽裝IP。客戶端將終止會話。

第二種情況是資料包來自內部網路中的客戶端並流向外部伺服器（防火牆之外）。 然後，RST被傳送到客戶端，RST源IP將成為伺服器的偽裝IP。

用於UDP會話

當可疑流量來自UDP作業階段時，WSA會執行類似的行為，但是L4TM不會傳送TCP RST，而是會傳送ICMP主機無法到達訊息（ICMP型別3代碼1）給使用者端或伺服器。但是，在這些情況下沒有IP欺騙，因為ICMP消息指出主機無法訪問，因此無法傳送資料包。在這種情況下，源IP將是WSA的IP。

這些RST和ICMP資料包使用資料路由表從WSA通過M1、P1或P2（具體取決於部署）傳送。